Lexmark PrintCryption™

(Firmware Version 1.3.0)

FIPS 140-2 Non-Proprietary
Security Policy

Level 1 Validation
Version 0.92

January, 2006

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Lexmark PrintCryption^TM from Lexmark International Inc. This Security Policy describes how the Lexmark PrintCryption^TM meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/cryptval/.

The Lexmark PrintCryption^TM is referred to in this document as PrintCryption, PrintCryption module, cryptographic module, firmware module, or module.

References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Lexmark International website (http://www.lexmark.com) contains information on the full line of products from Lexmark International.

- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Lexmark International Inc. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Lexmark and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Lexmark International.

LEXMARK PRINTCRYPTION^{TM}

Overview

The Lexmark PrintCryption^{TM} is an option for the Lexmark printers that enable the transfer and printing of encrypted print jobs. This new Lexmark technology offers a level of security that is the first of its kind in the printing industry. With the PrintCryption module installed, the printer is capable of decrypting print jobs encrypted with the AES (FIPS 197) algorithm. The Lexmark PrintCryption^{TM} analyses the encrypted data stream, determines if the correct key was used to encrypt the data, decrypts the data and allows the confidential document to be printed. This new level of printing security is ideal for industries that commonly handle sensitive or personal information, such as financial institutions, government agencies, and healthcare organizations.

Module Specification

The PrintCryption^{TM} module is a firmware module composed of two executable binaries, and it is installed in Lexmark printers using a Downloaded Emulator Card (DLE), a serial interface PCB board that plugs into the printer. The DLE card is shown in Figure 1.
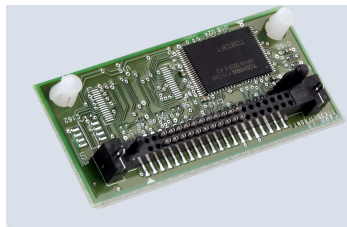
Figure 1 - DLE Firmware Card

Per FIPS PUB 140-2, the cryptographic module is classified as multi-chip standalone cryptographic module. The module meets overall level 1 FIPS 140-2 requirements, as detailed in Table 1.

Tested DLE Configurations (Option P/N15A1962):

T63x: DLE P/N 10G0149; C76x: P/N 16N3204; W820: P/N 19E0123; and C912: P/N 12N1253

Operating System: Lexmark proprietary ver. 2.4 based on Linux

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

Table 1 – Security Level per FIPS 140-2 Section

Logically, the cryptographic boundary is composed of two executable binaries and is evaluated for use on Lexmark printers that are running Linux operating system. Once the PrintCryption firmware is installed in the printer, the printer must use this firmware. The cryptographic module cannot be bypassed. Functionality is then controlled by the PrintCryption firmware.
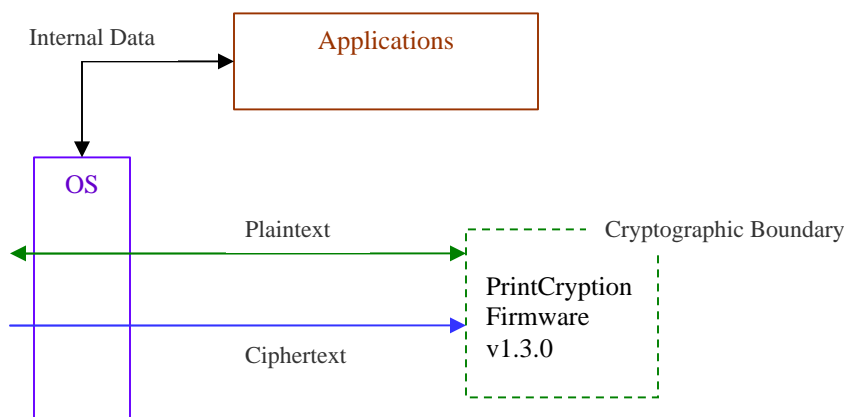
Figure 2 - Logical Cryptographic Boundary

The PrintCryption module is evaluated and tested on Lexmark printers including mono-color printers (T630, T632, and T634), Color printers (C760, C762, C912) and MFP printers (W820). The module's physical cryptographic boundary is the metal and plastic enclosure of the printer.
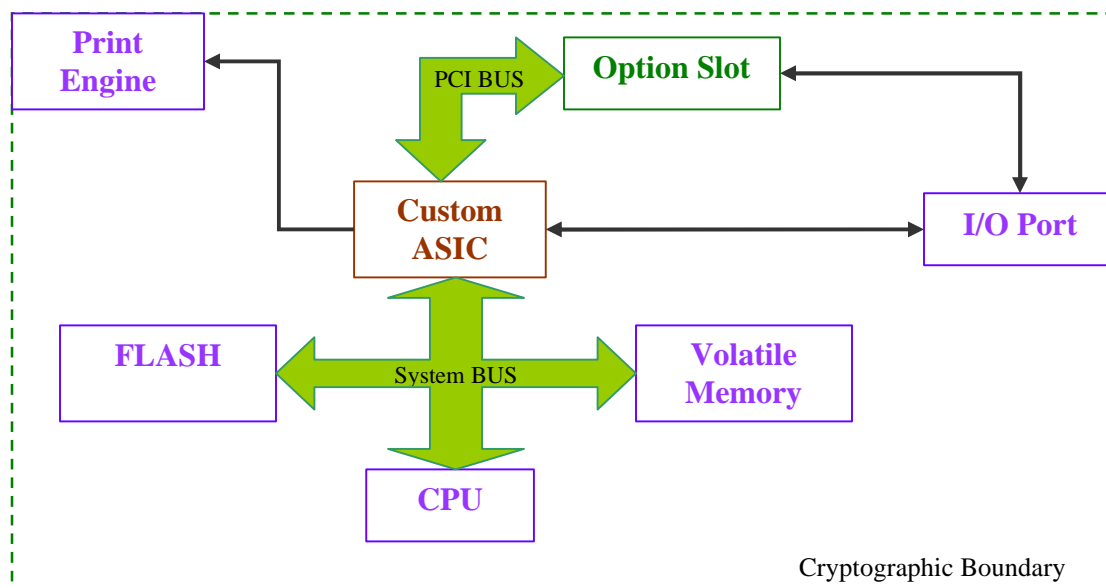
Figure 3 - Physical Cryptographic Boundary

Module Interfaces

The cryptographic module's physical ports are composed of the physical ports provided by the hardware platforms listed above. These printer ports include the network port, parallel port, USB port, paper exit port, multipurpose feeder, LED, and LCD display.

Since, all of the module's services are server processes, the logical interfaces of the module are network port and API calls, which provide the only means of accessing the module's services. Data inputs are service requests on the TCP ports. Control inputs are also data at TCP/IP port, however they are logically distinct from Data input and controls how the function is executed. The data output from the module includes X.509 certificate and deciphered data, which exit through the network port and an internal API, respectively. The status outputs of the module are sent via network and stored in log file.

All of these physical ports are separated into logical interfaces defined by FIPS 140-2, as described in the following table.

Logical Interface of the Module	Module Physical Port	FIPS 140-2 Logical Interface
Network Port	Network (Ethernet 10/100) Port USB Port Parallel Port	Data Input Interface
Network Port Internal API	Network (Ethernet 10/100) Port Paper Exit Port	Data Output Interface

Logical Interface of the Module	Module Physical Port	FIPS 140-2 Logical Interface
Network Port	Operator Panel Network (Ethernet 10/100) Port USB Port Parallel Port Paper Exit Port Multipurpose/envelope Feeder Power Switch Circuit Breaker Switch	Control Input Interface
Network Port Log File	LED LCD Display Network (Ethernet 10/100) Port USB Port Parallel Port.	Status Output Interface
Not Applicable	Power Plug Power Connector	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

Roles and Services

The module supports two roles, a Crypto Officer role and a User role, and an operator on the module must assume one of the roles. Descriptions and responsibilities for the two roles are described below.

Crypto Officer Role

The Crypto Officer installs and uninstalls the PrintCryption. The Crypto Officer is also responsible for monitoring the printer's configuration and operational status via network port.

Service	Description	Input	Output	CSP	Type of Access to CSP
Install	Assemble the printer(s); Install PrintCryption^{TM} firmware card; Install printer driver on host PC	Command	Result of installation	None	--
Uninstall	Uninstall the firmware	Command	Uninstalled module	None	--
Monitor	Configure of the module	Command	Module setting	None	--
Run Self-Test	Perform the self-test on demand	Command	Status output	Integrity Check Key	Read
Show Status	Call a show status from the printer status menu (HTTP) which has an LPC log page	Command	Status output	None	--

Table 3 – Crypto Officer Services, Descriptions, CSPs

Users utilize the cryptographic functionalities of the PrintCryption, and they communicate with the module via network port only.

Service descriptions and inputs/outputs are listed in the following table:

Service	Role	Input	Output	CSP	Type of Access to CSP
Public Key request	Users request for printers public key. The module generates a key pair if needed	Public Key Request (PKR) at network port 9150.	X.509 certificate	RSA public key	Read/Write
Secure Printing	AES encrypted printing program; Decrypts and prints the print job data using the supplied AES Session key	Encrypted print job at TCP/IP port 9152.	Status output	AES session key	Read/Write

Table 4 – User Services, Descriptions, Inputs and Outputs

Physical Security

In FIPS terminology, the firmware module is defined as a multi-chip standalone cryptographic module. The module runs on Lexmark printers listed in *Module Specification* section. The printers are made of all production-grade components and are enclosed in a strong plastic and steel case, which surrounds all of the module's internal components, including all hardware and firmware.

While purely a firmware module, the FIPS 140-2 evaluated platforms must have been tested for and meet applicable FCC EMI and EMC requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

Operational Environment

The operational environment is non-modifiable and thus not applicable for this firmware module. The PrintCryption module runs on the Linux OS, and configured for single-user mode by default. The operating system is used as an embedded OS within the Lexmark printers, and there is no direct access to the OS provided.

Cryptographic Key Management

The module implements the following FIPS-approved algorithms.

- AES ECB, CBC mode decryption – FIPS 197 (certificate #273, #274, #275, #276, #277)

- Deterministic Random Number Generator (RNG) – Appendix A.2.4 of ANSI X9.31 (certificate #100, #101, #102, #103, #104)

- HMAC– FIPS 198 (certificate #89, #90, #91, #92, #93)

- RSA (sign/verify) – PKCS#1 (certificate #73, #74, #75, #76, #77)

- SHS – FIPS 180-2 (certificate #350, #351, #352, #353, #354)

- TDES 2 key ECB mode encryption/decryption – FIPS 46-3 (certificate #356, #357, #358, #359, #360) (Note: The FIPS approved X9.31 Appendix A.2.4 PRNG utilizes 2 key TDES algorithm).

Additionally, the module utilizes the following non-FIPS-approved algorithm implementation:

- RSA Key Wrapping (PKCS #1): Key establishment method uses a 1024-bit key length providing 80-bits of security.

The module supports the following critical security parameters:

Key or CSP	Key type	Generation	Storage	Use
AES Session Key	128, 192, 256 bits AES key	Externally generated. Imported in encrypted form (RSA key transport)	Held in volatile memory in plaintext. Zerorized after the session is closed or on reboot.	Decrypts input data for printing
RSA Public Key	1024 bit RSA public key (80-bits of security)	Internally generated using PKCS#1 key generation mechanism	Stored on flash in plaintext. Zerorized by overwriting the flash image.	Key transport
RSA Private Key	1024 bit RSA private key (80-bits of security)	Internally generated using PKCS#1 key generation mechanism	Stored on flash in plaintext. Zerorized by overwriting the flash image.	Key transport
Integrity Check Keys	HMAC keys	Externally generated, hard coded in the module	Stored on flash in plaintext. Zerorized by overwriting the flash image.	Firmware Integrity test
X9.31 PRNG	2-key TDES keys, 8 bytes of seed value	Internally generated	Held in volatile memory only in plaintext. Zerorized on reboot.	RNG

Table 5 – Listing of Key and Critical Security Parameters

Access Control Policy

User functionalities have read/write access to the AES Session Key and RSA public key. AES Session key is used to decrypt the data for printing. RSA public key is used for AES Session key transport. Integrity Check Keys can be read by Crypto-Officer "Run Self-Test" service.

Key Generation

The module key is generated internally is 1024 bits RSA key pair using PKCS#1-compliant key generation techniques. FIPS-approved PRNG X9.31 Appendix A.2.4 is used to seed the RSA key generation mechanism. AES Session Key is generated outside of the module and imported via RSA key transport.

Key Storage

The AES Session Key is held in volatile memory only in plaintext. The RSA public key is stored in flash memory in an X.509 certificate in plaintext, and the RSA private key is stored flash memory in plaintext.

Key Entry and Output

All keys that are entered into (AES key) or output from (RSA certificate) the module are electronically entered or output. AES Session Key is enters into the module transported (encrypted) by RSA public key.

Key Zerorization

AES Session key is an ephemeral key which is zerorized after the connection is closed or by rebooting the module. The module provides no service to erase or discard the RSA key pair. The key pair is erased by overwriting the flash image with a new image.

Self-Tests

The PrintCryption module runs power-up and conditional self-tests to verify that it is functioning properly. Power-up self-tests are performed during startup of the module, and conditional self-tests are executed whenever specific conditions are met.

Firmware Integrity Check: The module employs a firmware integrity test in the form of HMAC SHA-1.

Cryptographic Algorithm Tests: Known Answer Tests (KATs) are run at power-up for the following algorithms:

- AES KAT
- TDES KAT
- RSA Sign/Verify and Encrypt/Decrypt pair-wise consistency check
- SHA-1 KAT
- X9.31 RNG KAT

The module implements the following Conditional self-tests:

- Continuous RNG Test for X9.31 PRNG

- Continuous RNG Test for entropy gathering
- RSA Sign/Verify and Encrypt/Decrypt pair-wise consistency check

If any of these self-tests fail, the module will output an error indicator and enter an error state.

Design Assurance

Source code and associated documentation files are managed and recorded using the ALS. ALS is a version control system that stores multiple revisions of the same file with a revisionary history and older versions are always accessible.

Additionally, Microsoft Visual Source Safe (VSS) version 6.0 is used to provide configuration management for the firmware module's FIPS documentation. This software provides access control, versioning, and logging.

Mitigation of Other Attacks

The PrintCryption module does not employ security mechanisms to mitigate specific attacks.

OPERATION IN FIPS MODE

The PrintCryption meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

Initial Setup

The DLE card containing PrintCryption module may be factory installed or user-installed. Lexmark provides an Installation sheet, a driver CD with publications, and license agreement for the module in the option kit.

Installation procedure of the module is as follows.

1. Print a menu settings page:

    a. Press **Menu** until **Utilities** menu appears, and then press **Select**.

    b. Press **Menu** until Print menu appears, and then press **Select** to print the page.

       Note: This Page is needed for later use.

    c. Configure the printer onto the TCP/IP network per installation requirements. If the printer is behind a firewall, it must allow IP ports 9150 and 9152 to pass through.

2. Turn off the printer and install the card. Please refer to the printer's documentation for further instructions on installing the card.

3. Turn the printer on.

    a. If the printer displays the message **41 – Unsupported Firmware Card**, then the installed card is not compatible for the printer. Turn off the printer and remove the card.

    b. If the printer displays the message **Resetting all of NVRAM** for longer than 45 seconds, turn off the printer and reinstall the card.

4. Print a menu settings page. If the new card is not listed under **Printer Information**, turn off the printer and repeat steps 2 and 3.

5. Launch the CD to host PC to install the software application using **setup.exe** program. Please refer to the documents on the CD for further instructions on installing the software. The setup executable, once launched, will:

    a. Ask for confirmation of the End-User License Agreement.

b. Present a small README, which explains that after installation, the Crypto Officer can add a new port to their printer driver that will support Lexmark PrintCryption^{TM}.

Note: Please refer to *Crypto Officer Guidance* section for more information.

c. Perform the installation, and stop and restart the print spooler.

6. Print a menu settings page. Compare these settings to those on the page printed in step 1.

7. Place the Option Added label on the printer next to the printer model and serial number label. Lexmark provide the **Option Added** label with the Installation guide.

Crypto Officer Guidance

The Crypto Officer is responsible for installing, uninstalling and monitoring the module. The card comes in a static sensitive package. Upon receiving the PrintCryption card, the Crypto Officer should check for any signs of tampering to the package, including a damaged seal or package.

The Crypto Officer may follow the installation sheet found in the option kit to install the PrintCryption module. After the installation is complete, the Crypto Officer must print a Menu page and verify that **16M Optional Firmware Card** is displayed under the **Installed Features** section of the Menu Page.

The Crypto Officer must configure the printer onto the TCP/IP network per installation requirements. While installing the PrintCryption host software application on a PC, Crypto Officer must choose **port 9150** to communicate with the printer. It is recommended that Crypto Officer name the port "FIPS" to clearly distinguish the port that provides secured printing service.

User Guidance

The User accesses the module printing functionality as a user over network. Although *outside the boundary* of the module, the User should be careful to use secured printing services as needed.

Users can select the AES encryption key length, block length and mode using the printer property.

1. Open the printer folder, right click on the desired printer and select **Properties**.

2. Navigate to **Port** tab and press the **Configure Port** button to proceed.

3. **Configure Secure Port** dialog box will appear which enables Users to choose their options.

Configure Secure Port   ✕

┌─ Port Settings ──────────────────────────────────────┐
│   │
│   Port Name: FIPS   │
│   │
│   Host Name/Address: 192.168.2.100   │
│   │
└───┘

┌─ AES Encryption Settings ────────────────────────────┐
│   │
│   Key Length (bits):   128   ▼   │
│   │
│   Block Length (bits):   128   ▼   │
│   │
│   Cipher Mode: ECB   ▼   │
│   │
│   ☑ Save As Default Settings │
│   │
└───┘

            [OK]   [Cancel]

Figure 4 - Configuring a Secure Port

Users must choose the key size and block size approved in FIPS PUB 197 standard. FIPS approved key and block sizes, and mode of operation are as follows:

- Key Length: 128, 192, or 256 bit.

- Block Length: 128 bit.

- Cipher Mode: ECB (Electronic Code Book, or CBC (Cipher Block Mode).

Setup.exe also installs Lexmark PrintCryption Utility (LPCU) program as part of the install session. The program can be invoke by -
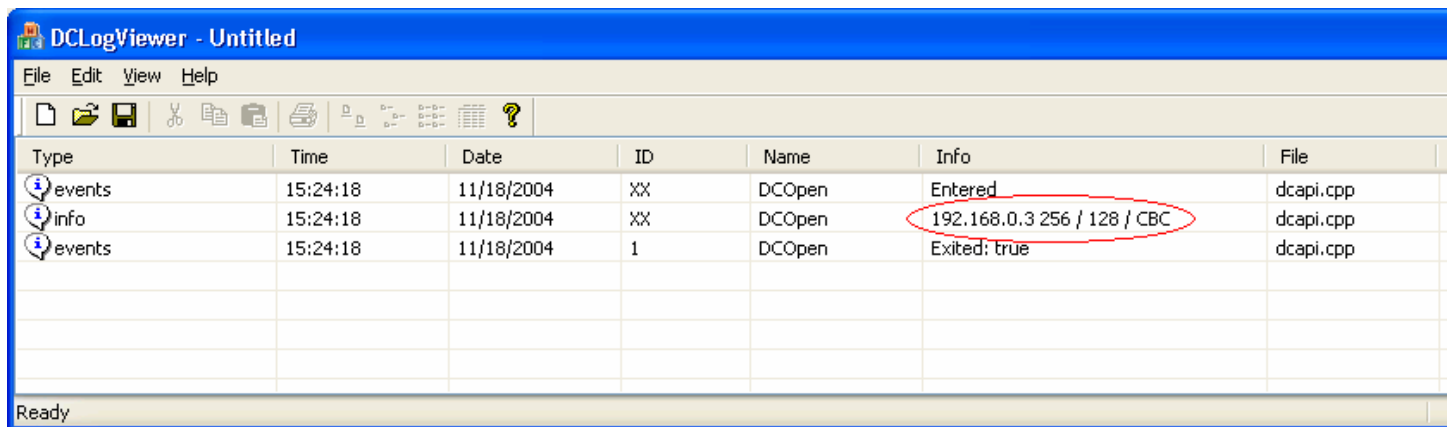
START → Programs → Lexmark → PrintCryption → PrintCryption Test Utility

The LPCU utility program can help Users to determine:

- The Lexmark PrintCryption Card is installed.

- The network path exists, even through a firewall, and when **ping** command does not work.

- The proper IP ports (9150 and 9152) are open.

- The printer is capable of returning an X.509 security certificate.

- The printer can successfully decode an encrypted packet.

Users also can view the communication to the printer via PrintCryption Log Viewer, installed during the installation session, which can be started by -

START → Programs → Lexmark → PrintCryption → PrintCryption Log Viewer

Figure 5 - PrintCryption Log Viewer

Users can see the key size, block length, and mode been used for encryption from the Log Viewer program.

ACRONYMS

AESSD	AES Session Daemon
ANSI	American National Standards Institute
API	Application Programming Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DKMD	Decryption Key Management Daemon
DLE	Downloaded Emulator Card
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash MAC
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
KAT	Known Answer Test
LED	Light Emitting Diode
LPC	Line Printer Control
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
PC	Personal Computer
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SKH	Session Key Header
SNMP	Simple Network Management Protocol
SP	Secure Platform
TCP	Transmission Control Protocol
VSS	Visual Source Safe